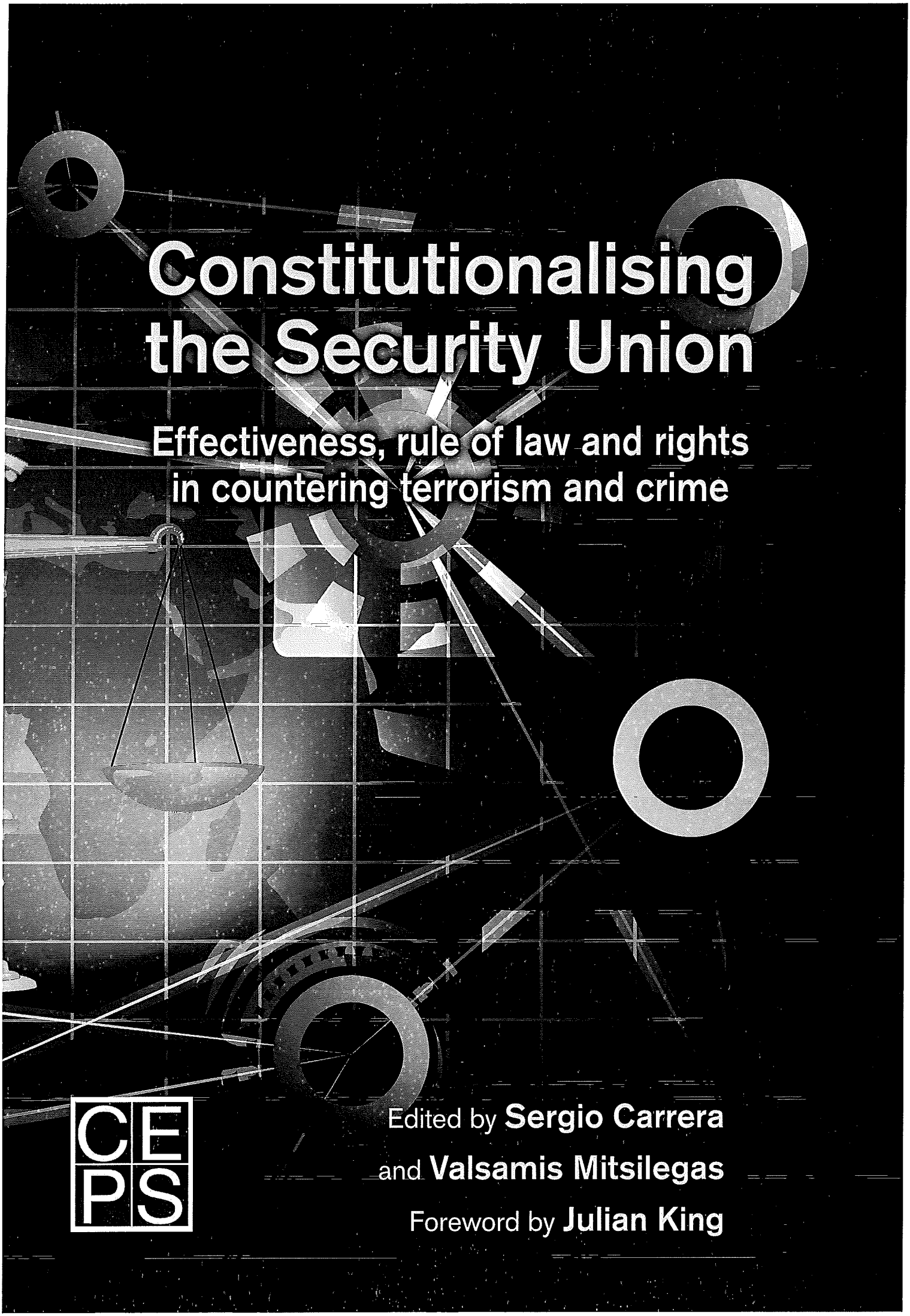
International cooperation and the exchange of personal data: Safeguarding trust and fundamental rights

Brouwer, E.R.

published in
Constitutionalising the Security Union
2017

document version
Publisher's PDF, also known as Version of record



Constitutionalising the Security Union

Effectiveness, rule of law and rights in countering terrorism and crime

Edited by **Sergio Carrera**
and **Valsamis Mitsilegas**
Foreword by **Julian King**

CEPS

CONSTITUTIONALISING THE SECURITY UNION

EFFECTIVENESS, RULE OF LAW AND RIGHTS IN COUNTERING TERRORISM AND CRIME

EDITED BY

SERGIO CARRERA

AND

VALSAMIS MITSILEGAS

FOREWORD BY

JULIAN KING

CENTRE FOR EUROPEAN POLICY STUDIES (CEPS)

BRUSSELS

CONTENTS

7. INTERNATIONAL COOPERATION AND THE EXCHANGE OF PERSONAL DATA: SAFEGUARDING TRUST AND FUNDAMENTAL RIGHTS

EVELIEN BROUWER

7.1 Introduction

Recurring terrorist attacks in cities in Europe, but also elsewhere, establish the necessity of timely and effective cooperation among the different authorities involved in preventing terrorism and serious crimes. This cooperation requires, first of all, mutual knowledge about the competent organisations or agencies in other states and the existing networks and contact channels between the states involved, to allow swift and reliable exchange of information. Second, in order to ensure the willingness to cooperate and to share information, international cooperation can only be based on mutual trust between these states. This trust concerns the reliability and accuracy of the information to be shared, but also the lawfulness of data processing and the protection of fundamental rights in the different states involved.

When dealing with the cooperation between EU states, mutual trust is considered a fundamental principle underlying such cooperation in the Area of Freedom, Security and Justice (AFSJ). Yet the case law of the Court of Justice of the European Union (CJEU) has underlined that even if trust with regard to the protection of fundamental rights and EU law can be assumed, there is no such principle of "blind trust".[1] In the case of evidence concerning

[1] See E. Brouwer and D. Gerard (eds), "Mapping Mutual Trust: Understanding and Framing the Role of Mutual Trust in EU Law", EUI Working Paper MWP 2016/13, European University Institute, Florence (http://cadmus.eui.eu/). See also the different contributions to the special section on "Mutual Recognition and Mutual Trust -

a breach in the protection of fundamental rights in another EU state, such evidence may rebut trust, and thus block cooperation, also with regard to the exchange of personal information.[2]

Whereas there is ongoing discussion about the threshold to apply for the evidence necessary to substantiate the 'rebuttable presumption' of mutual trust between EU states, it seems clear that when dealing with cooperation between the EU and third states, this threshold must certainly be lower. Unlike within the EU, the cooperation between the EU and third states is not built upon shared values and fundamental principles, the harmonisation of law and procedural guarantees, or mechanisms for cooperation and supervision. Therefore, as underlined by the CJEU in the case law described below, the adoption of agreements with third countries, and more specifically agreements on data sharing, must include further and more detailed rules on the protection of fundamental rights.

Since the terrorist attacks in the US in September 2001, many instruments have been adopted within the legal framework of the EU dealing with the collection and exchange of personal information. Aside from those resulting in large-scale data collection on third-country nationals (such as the Schengen Information System (SIS) II, Visa Information System (VIS) and Eurodac), these measures also involve the exchange of information between judicial and law enforcement authorities (through Europol, Eurojust and the Prüm Treaty) and the adoption of agreements on data transfers between the EU and third states. The cooperation between the EU and third states involves among others the exchange of passenger data with the US, Canada and Australia, and cooperation between the US government and Europol for the purpose of the Terrorist Financing Tracking Program (TFTP).[3] During the negotiations preceding the adoption of these

---

Reinforcing EU Integration?", in *European Papers – A Journal on Law and Integration*, Vol. 1, No. 3, 2016, and Vol. 2, No. 1, 2017.

[2] Already in 2006, the CJEU found that with regard to entry bans reported in the Schengen Information System (SIS), the refusal of entry to third-country nationals who were spouses of EU citizens could not automatically be based on the SIS information, but required the further exchange of information between the reporting and the executing state. See CJEU, Judgment of the Court (Grand Chamber) of 31 January 2006 in Case C-503/03, *Commission* v *Kingdom of Spain*.

[3] An analysis of many of these measures is provided in D. Bigo, E. Brouwer, S. Carrera, E. Guild, E.-P. Guittet, J. Jeandesboz, F. Ragazzi and A. Scherrer, "The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty

agreements, concerns were raised by the European Parliament, different non-governmental organisations, and the national and EU supervisory data-protection authorities, addressing the level of data protection in the third state and the scope of legal protection of the data subjects involved. Because of these concerns, together with the scrutinising role of the CJEU (on the basis of which, for example, the EU–US Agreement on Passenger Name Records (PNR) of 2004 was annulled), the negotiations on these agreements were painstakingly long, requiring both a diplomatic and a stringent position by the European Commission.[4] The adoption in December 2016 of the EU–US Umbrella Agreement, entering into force in February 2017, was presented by Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, as a "common transatlantic privacy framework based on high standards with the USA", supporting and facilitating "law enforcement cooperation by building trust and legal certainty for data transfers".[5]

In case law dealing with the mass collection of personal data and data transfer to third states, the CJEU has defined important criteria that, as argued above, at least should be taken into account when dealing with agreements on the transfer of personal data between third states and the EU.[6] On the basis of this case law and the new EU data protection rules entering into force in 2018, this chapter will address the following standards: necessity and proportionality, transparency or the principle of purpose limitation, and the right to legal remedies. It will submit that these standards

---

Agenda", CEPS Policy Brief No. 81, Centre for European Policy Studies, Brussels, February 2015.

[4] See CJEU, Judgment of the Court (Grand Chamber) of 30 May 2006 in Joined Cases C-317/04 and C-318/04, *European Parliament* v *Council and Commission*, annulling Decision 2004/496/EC – Agreement between the European Community and the United States of America – Passenger Name Records of air passengers transferred to the United States Bureau of Customs and Border Protection (adopted on the wrong legal basis, Art. 95 EC, on the internal market). See also the new Agreement of 14 December 2011, published in OJ L 215/5, 11.8.2012.

[5] See V. Jourová, "EU–US data flows and data protection: Opportunities and challenges in the digital era", speech delivered in Washington, D.C. on 31 March 2017 (SPEECH/17/826), Press Release, European Commission, Brussels.

[6] See also on the implications of the CJEU's case law in I. Nesterova, "Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards", ESIL Conference Paper No. 11/2016, European Society of International Law Annual Conference in Riga, 8–10 September 2016 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2911999&download=yes).

should be the among the guiding principles during, but also before starting negotiations with a third state for the purpose of sharing personal information. Furthermore, the chapter will address some lack of clarity and possible gaps in protection under the Umbrella Agreement, also taking into account the risks of onward transfers by the third state to other non-EU states.

7.2 Necessity and proportionality

In early case law, the European Court of Human Rights (ECtHR) made clear that the collection, storage and processing of personal information falls within the scope of the right to privacy as protected in Art. 8 of the European Convention on Human Rights (ECHR), irrespective of whether this information is subsequently used or not.[7] Art. 8(2) ECHR prescribes that every limitation to the right to privacy should be in accordance with the law and necessary in a democratic society for one of the goals specified in Art. 8(2). In EU law, the right to privacy has been included in Art. 7 of the EU Charter of Fundamental Rights, and read together with Art. 52(1) of the Charter, these provisions further require that each limitation should be in accordance with the principle of proportionality.

According to the General Data Protection Regulation (GDPR) of 2016, which will be applicable from 2018, the processing of personal data shall only be lawful for the grounds specified in its Art. 6.[8] Dealing with the execution of public tasks, this provision entails that the processing must be "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". Except for the situations described in para. 2, Art. 9 prohibits the processing of special categories of personal data, such as racial or ethnic origin, religious or philosophical belief and biometric data. Furthermore, the Data Protection Directive 2016/680 dealing with the processing of data for law enforcement purposes and which was to be implemented in 2016, provides in Arts 35-40

---

[7] ECtHR, *Amann* v *Switzerland*, Application no. 27798/95, 16 February 2000.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, 4.5.2016.

further requirements specifically dealing with the transfer of personal data to third states.[9]

The aforementioned conditions on data transfers to third states must be read and applied in conformity with the fundamental rights of privacy and data protection and the criteria defined on the basis of these rights by the ECtHR and the CJEU. More specifically, the conclusions formulated by the CJEU in the cases of *Digital Rights Ireland* in 2014 and *Schrems* in 2015 should be considered basic criteria to be fulfilled by the EU legislator whenever negotiating agreements with third states.[10] In the judgment in *Digital Rights Ireland*, the CJEU annulled the Data Retention Directive 2006/24, because its implementation would risk violating the rights in Arts 7 and 8 of the Charter. In its case law, the CJEU referred explicitly to the case law of the ECtHR, dealing with Art. 8 ECHR.[11]

In its judgment in *Digital Rights Ireland*, the reasons the CJEU gave for finding the Data Retention Directive in violation of Arts 7 and 8 of the Charter were related to the following grounds.[12] First, the Directive was not considered in compliance with the principle of proportionality, as it would entail processing the data of practically the entire European population, involving persons without any link to criminal prosecution. Second, the Directive did not include prior review by a court or independent body to determine whether access is strictly necessary. Third, the CJEU found that the Directive established a "general absence of limits" with regard to authorities having access to data and subsequent use, or abuse. Fourth, the time limits as provided in the Directive would not be circumscribed to what is strictly necessary.

Applying these standards to third-country agreements, such as the Umbrella Agreement, but also to future agreements, this means that at the least the following criteria must be met, taking into account the principle of

---

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119/89, 4.5.2016.

[10] See CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014 in Case C-293/12, *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others*; see also CJEU, Judgment of the Court (Grand Chamber) of 6 October 2015 in C-362/14, *Maximillian Schrems* v *Data Protection Commissioner*.

[11] See Case C-293/12 (*supra*), paras 35 and 55.

[12] Ibid., paras 57-68.

necessity and proportionality. They should not include provisions allowing for the blanket and unspecified processing or transfer of personal information, involving large groups of citizens without any link to an individual suspicion or criminal investigation. Prior to the adoption of the agreement, the national and European data protection supervisors must be involved, assessing the necessity of the measure at stake. Furthermore, the agreement must provide specified and clear rules, limiting both the data retention of processed data, as well as the access and use by authorities, to what is strictly necessary. This latter requirement is closely related to the principle of purpose limitation, which is developed further in the next section.

7.3 Purpose limitation – Transparency

The requirement of transparency when dealing with data collection and data sharing follows not only from the right to privacy as included in Art. 8 ECHR and Art. 7 of the Charter, but is also to be considered one of the central principles of data protection law: the principle of purpose limitation.[13] Within the context of EU law, the right to data protection has been recognised as a separate fundamental right in Art. 8 of the Charter. The explicit inclusion of the principle of purpose limitation in Art. 8(2) of the Charter underlines that this is to be regarded as an intrinsic part of the right of data protection.

The principle of purpose limitation is included in Arts 5(1)(b) and 6 of the GDPR. According to Art. 5(1)(b), personal data may only be collected for "specific, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes". Furthermore, Art. 5(1)(c) of the GDPR explicitly refers to the principle of data minimisation, providing that personal data should be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed".

Elsewhere, we have described the different layers of the principle of purpose limitation, including the ban on "aimless data collection" and the obligation of purpose specification.[14] The first entails a material limitation of

---

[13] See Art. 5 of the Data Protection Convention of the Council of Europe of 28 January 1981, ETS, No. 108.

[14] E. Brouwer, "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation", in L.F.M. Besselink, F. Pennings and S. Prechal (eds), *The Eclipse of Legality Principle in the European Union*, Alphen aan de Rijn: Kluwer Law International, 2011, pp. 273-294.

the power to collect and process personal information, the second is an obligation to lay down in clear and transparent rules which data are to be collected or processed for which purposes. In different judgments, the ECtHR has clarified that "in accordance with the law", as stipulated as a condition in Art. 8(2) ECHR, means that the law allowing the use or collection of personal information must be accessible to the individual concerned and its consequences predictable.[15]

Dealing with the use of secret police files by the Swedish special police service in the famous *Leander* case, the ECtHR recognised that in cases of national security, the requirement of predictability cannot be the same as that applied to general cases.[16] However, the ECtHR made clear that "the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which, and the conditions on which, the public authorities are empowered to this secret and potentially dangerous interference to private life".

In 2008, assessing the UK's Interception of Communication Act in the *Liberty* v *UK* judgment, the ECtHR explicitly rejected the government's submission that when considering the requirement of a specific and clear legal basis, there would be a difference between intercepting the communication of targeted individuals and general surveillance schemes. More specifically, "[t]he Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other".[17]

Unlike its predecessor, Directive 95/46/EC, the GDPR does not refer explicitly to the right to privacy, nor to Art. 8 ECHR. However, Art. 1(2) specifies that this Regulation "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data". In different decisions, the CJEU has underlined the close relationship between the right to privacy and data protection.[18] The necessary condition

---

[15] See ECtHR, *Huvig and Kruslin* v *France*, Application nos 11801/85 and 11105/84, 24 April 1990, and *Malone* v *UK*, Application no. 8691/79, 2 August 1984.

[16] ECtHR, *Leander* v *Sweden*, 26 March 1987, paras 50-51.

[17] ECtHR, *Liberty* v *UK*, Application no. 58243/00, 1 July 2008, para. 61-63.

[18] CJEU, Judgment of the Court of 20 May 2003 in Cases C-465/00, *Rechnungshof* v *Österreichischer Rundfunk and Others*, and *Christa Neukomm* (C-138/01) and *Joseph Lauermann* (C-139/01), paras 68-71.

of transparent and specified rules, following from the protection of Arts 7 and 8 of the Charter, was underlined by the CJEU in its judgment in *Digital Rights Ireland*, in which the CJEU invalidated the Data Retention Directive.[19] According to the CJEU,

> the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.

Referring to earlier case law of the ECtHR applying Art. 8 ECHR, the CJEU stressed that the "need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data".

The aforementioned principles, and interpretation by the CJEU, imply that new instruments for data processing and data sharing, including agreements with third states, must provide clear rules defining the scope and content of the powers at stake. Furthermore, purpose limitation prohibits the blanket and unspecified sharing of data between authorities in the EU, and between the EU and third states. This also requires using precise definitions, and ensuring a harmonised interpretation and implementation of mutual agreements. For example, when including definitions for terms such as 'terrorist events' or 'serious crimes', if not further defined, these terms may be considered too vague and too open for a different interpretation to provide a sufficient and reliable basis for mutual exchange of information. Even if lower standards with regard to predictability may apply when it comes to internal security measures, the ECtHR made clear that both the circumstances and the conditions on the basis of which personal information may be processed for these purposes should be 'sufficiently clear'. Dealing with third-country agreements where the risk of unlawful access might be larger, further safeguards are necessary.

Finally, EU agreements with third states must be adopted on a clear legal basis and published in official journals, and substantive information

---

[19] See *Digital Rights Ireland* (Case C-293/12), op. cit., paras 54-55, where the CJEU also refers to the judgments of the ECtHR dealing with Art. 8 ECHR, including the *Liberty* v *UK* judgment.

with regard to the scope and implementation of third-country agreements should be submitted to the European Parliament and national parliaments. Only this allows parliaments and individuals to assess the legality of an agreement and prevents a lack of clarity about which state or organisation is to be held accountable for the implementation of the agreement.[20]

7.4 Access to effective legal remedies

The right to an effective judicial remedy is protected in Art. 47 of the Charter and more specifically with regard to data processing in Art. 79 of the GDPR.[21] In addition, dealing with data relating to criminal convictions and offences "or related security measures", Art. 10 of the GDPR provides that this data processing may only be carried out "under the control of official authority" or when the processing is authorised by EU or national law providing for "appropriate safeguards for the rights and freedoms of data subjects". The GDPR provides for a more extended role of national supervisory authorities and the European Data Protection Supervisory Board (replacing the current European Data Protection Supervisor).

In the *Schrems* judgment, the CJEU emphasised the importance of the right to effective judicial protection:

> legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very

---

[20] That is to avoid a gap of legal protection as recently established in view of the EU-Turkey deal on the relocation of asylum seekers from the EU to Turkey and vice versa. Here, the General Court declared itself not competent to assess the human rights implications of this agreement, considering it was not an EU treaty – see the Order of the General Court of 28 February 2017 in Case T-192/16, *NF* v *European Council*.

[21] Art. 79 of the GDPR states that "each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation".

> existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.[22]

Furthermore, in *Digital Rights Ireland*, when annulling the Data Retention Directive because of violation of Arts 7 and 8 of the Charter, the CJEU scrutinised the lack of access to any independent review. According to the CJEU,

> the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.[23]

Moreover, the CJEU found that

> it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security ... is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.[24]

In other words, the CJEU regarded the lack of independent control and safeguards ensuring the security and compliance with data protection rules in a third state to which personal data would be transferred from controllers or authorities within the EU, as a violation of Art. 8 of the Charter.

Considering the EU-US Umbrella Agreement, it is questionable whether the individual right of access to legal remedies and the supervisory role of data protection authorities is sufficiently and effectively safeguarded. In the first place, the scope of protection provided by the Umbrella Agreement seems to be limited. This Agreement has been approved by EU negotiators under the condition of the US legislator adopting the Judicial

---

[22] See *Schrems* (Case C-362/14), op. cit., para. 95.

[23] See *Digital Rights Ireland* (Case C-293/12), op. cit., para. 62.

[24] Ibid., para. 68.

Redress Act, as this would ensure that data subjects whose data would be transferred from the EU to the US would have access to legal remedies.

However, the text of the Judicial Redress Act, adopted in February 2016 by the US Congress, only offers citizens of designated countries access to civil remedies, in accordance with the US Privacy Act of 1974, and this list just includes EU states (with the exception of Denmark and the UK).[25] Therefore, third-country nationals resident in the EU, or third-country nationals whose data have been collected by EU authorities (e.g. in SIS II, Eurodac or the VIS) and subsequently transferred to US authorities, are not covered by this right to judicial remedies.

Second, the US Privacy Act and the Judicial Redress Act provide access to civil law procedures, but not legal redress actions in the field of criminal or administrative law. This means that formally, whenever measures are taken in immigration or criminal law procedures against EU citizens whose data have been transferred under the Umbrella Agreement, these individuals may be excluded from access to legal remedies, or their procedural rights may be limited by US law. In this regard, the rules in the Umbrella Agreement differ from the specific provisions included in the EU-US TFTP Agreement of 2010, which provides for "all persons regardless of nationality or residence, access to judicial redress from adverse administrative action". Also, the EU-US PNR Agreement includes a wider scope of legal protection in Art. 13(1), providing that "any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with US law". Furthermore, Art. 13(2) provides that "any individual is entitled to seek to administratively challenge the Department of Homeland Security (DHS) decisions related to the use and processing of PNR". Where these provisions seem to bridge the aforementioned gap of the Judicial Redress Act, the relationship between the general rules of the Umbrella Agreement and the rules in the specific transfer agreements should be made clearer, also when adopting future agreements.

Finally, the effect of the executive order under the Trump administration of 25 January 2017 ("Enhancing Public Safety in the Interior

---

[25] The Judicial Redress Act requires the adoption of a separate list of 'designated countries', to be found on the US Department of Justice website (http://www.justice.gov/opcl/judicial-redress-act-2015). This list excludes Denmark and the UK, awaiting the formal notification that these countries shall apply the Umbrella Agreement.

of the United States") requires further investigation. According to section 14 of the Privacy Act, as amended by this executive order, "[a]gencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information".[26] Although the phrase "to the extent consistent with applicable law" may limit the practical outcome of this executive order, the text itself seems to imply that the former extension of rights in the US Privacy Act to EU citizens by the adoption of the Judicial Redress Act should be considered void.

7.5 Adequacy decision, appropriate level of data protection and onward transfer to third states

In *Schrems* v *Data Protection Commissioner*, the CJEU annulled the Safe Harbour Decision 2000/520, in which the Commission had found that US law provided an adequate level of data protection in accordance with Directive 95/46, allowing the transfer of personal data from the EU to organisations within the US. In this judgment, the CJEU defined "an adequate level of data protection" as a level of protection that is "essentially equivalent protection to that guaranteed within the European Union".[27] Even if the means chosen by a third state to ensure an adequate level of protection might differ from those employed in the EU, the CJEU found that those means must nevertheless "prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union".

Therefore, "essentially equivalent" would mean that the essential elements of data protection included in Art. 8 of the Charter are to be complied with. This, according to the CJEU, also implies that, "as the level of protection ensured by a third state is liable to change", the Commission should periodically assess the content of those rules to ensure that the

---

[26] See "Executive Order: Enhancing Public Safety in the Interior of the United States", Office of the Press Secretary, White House, Washington, D.C., 25 January 2017 (https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united).

[27] See *Schrems* (Case C-362/14), op. cit., para. 74.

decision with regard to the adequate level of data protection is still factually and legally justified.[28]

In accordance with Art. 45 of the GDPR (and Art. 36 of Directive 2016/680), the transfer of personal data to a third country or an international organisation requires a prior adequacy decision by the Commission. This decision can only be based on an assessment of the adequacy of protection in that third state or organisation with regard to, among others, the rule of law, respect for human rights and fundamental freedoms, as well as "effective and enforceable data subject rights and effective administrative and judicial redress for the data subject at stake". In the absence of such a decision, Art. 46 of the GDPR (and Art. 37 of Directive 2016/680) allows personal data to be transferred to a third country or international organisation, but only if the processor or controller provides "appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available".

Considering this general requirement of either an adequacy decision or the provision of an appropriate level of protection necessary for the transfer of data from the EU to third states, it seems odd that the Umbrella Agreement allows in Art. 7 the onward transfer of personal data, acquired on the basis of this Agreement between the EU and the US, to other third states, only if the prior consent of the state originally transferring this data has been obtained. The Umbrella Agreement does not provide, through a decision on the adequate level of data protection in the US, for this onward transfer, but refers in Art. 7(2) to "an appropriate level of protection of personal information", which should be ensured in the third state.[29] Furthermore, Art. 7(2) provides that the transfer "may" be subjected to specific conditions. In other words, the onward transfer of data to third states on the basis of the Umbrella Agreement is bound by fewer guarantees and safeguards than those provided in the GDPR and Directive 2016/680 for the transfer of personal data from the EU to third states in general.

7.6 Concluding remarks

The negotiation of agreements with third states allowing the transfer of personal data should be based on evidence sustaining the necessity and

---

[28] Ibid., para. 76.

[29] See also the Note on the EU-US Umbrella Agreement by the Meijers Committee, CM1613, Utrecht, 2016 (www.commissie-meijers.nl).

proportionality of any systematic and general data transfers. In this regard, it should be taken into account that the GDPR and Directive 2016/680 already provide a basis for the exchange of personal data in individual and specific situations, under conditions and supervision by data protection authorities. The adoption of any new agreements with a third state allowing for the further and more general exchange of personal data requires a prior and in-depth examination of the law, practice and judicial redress systems in that state.

Furthermore, the level of protection should be in accordance with the criteria developed in the aforementioned case law of the CJEU and "essentially equivalent" to the protection offered by the GDPR and the Directive. Any future agreement must have a clear legal basis and be officially published to ensure its transparency and the accountability of the powers and actors involved. Finally, in dealing with the Umbrella Agreement, the EU legislator should address the current gap in protection for non-EU citizens with regard to the right to- judicial remedies and the lack of specific safeguards for the onward transfer of data to third states.